حوكمة تكنولوجيا المعلومات على مخاطر المعاملات الإليكترونية

Information technology governance on the risks of electronic transactions

عبد السلام محمد مخلوف

جامعة السلطان زين العابدين(ماليزيا) ، البريد الالكتروني: Rotwan603@gmail.com

تاريخ الاستلام: 2021/07/21 تاريخ القبول: 2021/09/10 تاريخ النشر: 2022/01/09

الملخَّص:

لقد أولت حوكمة تقنية المعلومات في المجال الإلكتروني اهتمامًا كبيرًا. حيث إنها المكون الأساسي لنجاح المعاملات الاقتصادية، بدايةً من الاقتصاد الصناعي إلى الاقتصاد الرقمي. وقد شهد في بداية الألفية الجديدة، بعد آخر في إنشاء شركات دولية الحماية تقوم بتشفير البيانات المنقولة بين الأطراف. وكذا وسائل لإثبات الهوية تشمل التوقيع الإلكتروني، من خلال تسليط الضوء على معالجة طرق حماية أطر الدفع الإلكتروني. ومن خلال تطوير نظام المعاملات الآمن، مع مراعاة أساسيات حماية الشبكات المحلية للشركات. عن طريق الاستعانة بالمنهج الوصفي والتحليلي لوصف تطور المعاملات الإليكترونية وتحليل بياناتها للوقوف على المخاطر الناتجة منها. واستنتاجنا من الدراسة: أن غالبية الدول قد طبقت سياستها الرامية إلى تطوير الكفاءات البشرية. حيث تقوم الهيئات العالمية المختصة في مجال المعلوماتية بتطوير برمجيات الحماية الإلكترونية وإعادة النظر في برامج التعليم العالي والتكوين المهني، في مجال تكنولوجيات الإعلام والاتصال. باستخدام أنظمة تشغيل محمية تقلل من المخاطر الإليكترونية. نتيجة الثورة الحاصلة في مجال المعلومات والمعرفة.

الكلمات الافتتاحية: حوكمة تكنولوجيا المعلومات – التشفير – التوقيع الإلكتروني – نظام المعاملات الإلكترونية الآمنة.

Abstract:

Information technology governance in the cyber field has given great attention. As it is the essential component of the success of economic transactions, from the industrial economy to the digital economy. At the beginning of the new millennium, it witnessed another dimension in the establishment of international protection companies that encrypt data transmitted between parties. As well as means to prove identity, including electronic signature, by highlighting the treatment of methods of protecting electronic payment frameworks. And through the development of a secure transaction system, taking into account the fundamentals of protecting companies' local networks. By using a descriptive and analytical approach to describe the development of electronic transactions and analyze their data to determine the risks resulting from them. Our conclusion from the study: The majority of countries have implemented their policy aimed at developing human competencies. Where international bodies specialized in the field of informatics are developing electronic protection software and reviewing higher education and professional training programs in the field of information and communication technologies. Using protected operating systems that reduce cyber risks. As a result of the revolution in the field of information and knowledge

Key Words: Information Technology Governance - Encryption - Electronic Signature - Secure Electronic Transaction System.

مقدمة:

أصبحت حوكمة تقنية المعلومات من الاهتمامات الرئيسية المنظمة للأعمال اليومية، خاصةً في ظل تأثيرات المتغيرات البيئية الجديدة وانعكاساتها. كما تحتوي على مخاطر تتعلق بأمن وسرية المعلومات التي يتم تبادلها بين الأطراف، أثناء إبرام المعاملات الإلكترونية، كا المعلومات أثناء تدفقها عبر الإنترنت حيث يمكن نقل المحتوى الخاص بهم وقراءته، كا المعلومات المالية (أرقام الحسابات وأرقام بطاقات الائتمان)، ويمكن أن تتعرض مواقع الويب الخاصة بالمؤسسات للقرصنة والتخريب من قبل "Internet Hackers". مما أدى إلى ضرورة اللجوء إلى مجموعة من الآليات والأنظمة التي توفر السرية والأمان والخصوصية.

لذلك ستُعنى هذه الدراسة بالمحاور الأتية:

1. حوكمة تكنولوجيا المعلومات.
2. التوقيع الإليكتروني والتشفير.
3. الشهادات الرقمية ونظام المعاملات الإلكترونية الآمن.

- **مشكلة البحث**

في ظل البحث عن خيارات وحلول تحمي العملاء من مخاطر التواجد في البيئة الإلكترونية، ومن أجل ضمان الحماية الكافية، تبرز معالم المشكلة بأنها: إلى أي مدى يمكن لحوكمة تقنية المعلومات أن تخلق آليات تحمي المعاملات الاقتصادية الإلكترونية؟ وهذا قادنا إلى تجزئة الاشكالية الأساسية إلى السؤالين الفرعيين **التاليين:**

- **أسئلة البحث**

1- كيف يمكن لآليات الحماية الإلكترونية أن تقلل من مخاطر الاحتيال والقرصنة المعاصرة؟

2- هل يعتمد مستقبل التعاملات الإلكترونية على مدى فاعلية ونجاح أساليب المنع التي توفرها حوكمة تقنية المعلومات؟

- **أهمية البحث:** تكمن أهمية البحث في:

أن مبدأ الأمن هو الخطوة الأولى في التعاملات التجارية الإلكترونية، وبدون ذلك لن تتمكن أطراف التعامل من التواجد في الدوائر الإلكترونية بسبب انعدام الثقة وانعدام الحماية مما يجعلها عرضة لمخاطر الاحتيال، و هذا ما يطرح مستقبل منظمات الأعمال أمام حافة الانهيار من جهة و إعاقة حركية التجارة و تراجع آليات التواصل بين المتعاملين من جهة أخرى ما يعني بعبارة أو أخرى تغيير إحداثيات الاقتصاد النظري إلى أقصى الحدود، ما قد يتسبب في وضع مصير منظمات الأعمال على محك الانهيار.

- **منهجية البحث** : يتبع الباحث في هذا البحث:

المنهج الوصفي والتحليلي لوصف تطور المعاملات الإليكترونية، وتحليل بيانتها للوقوف على تقليل المخاطر الناتجة منها.

- **فرضيات البحث:**

- العمل بتصميم وتطوير برمجيات الحماية الإلكترونية، للتعامل مع مخاطر الاحتيال والقرصنة المعاصرة. عن طريق منظمات دولية متخصصة في مجال المعلوماتية.
- يعتمد مستقبل المعاملات الاقتصادية في الدوائر الإلكترونية على فعالية وكفاءة أساليب الوقاية الحديثة، حيث إن عنصر الأمن هو الركيزة الأساسية لإجراء المبادلات التجارية والقيام بعمليات التسوية.

- **حوكمة تكنولوجيا المعلومات**

1. **مفهوم حوكمة تكنولوجيا المعلومات:**

تتعدد و تتنوع تعاريف حوكمة تكنولوجيا المعلومات ،فقد قدم معهد حوكمة تكنولوجيا المعلومات ITGI تعريفاً لحوكمة تكنولوجيا المعلومات في سنة 2003 و هو " أن حوكمة تكنولوجيا المعلومات هي مسؤولية مجلس الادارة، و الادارة التنفيذية، و هي جزءاً مكملا لحوكمة المشروعات و تتألف من القيادات و الهيكليات التنظيمية و العمليات التي تتضمن أن تكنولوجيا المعلومات المنظمة تساند و تبرز أهداف و استراتيجيات المنشاة " (عوض, أمال محمد، 2008). بينما يرى أحد الباحثين أنها: "وسيلة أو أداة فعالة في المنشاة من خلال خلق مرونة في تكنولوجيا المعلومات و في هيكليات و عمليات نظم المعلومات حيث ينظر إليها على أنها القدرة التنظيمية لرقابة تركيب و تطبيق استراتيجية تكنولوجيا المعلومات و تعتبر دليل للاتجاه المناسب بغرض تحقيق ميزة تناسبية للمنشاة". (عبدالرحمن, نجلاء إبراهيم يحيي، 2013) ومن التعاريف السابقة يرى الباحثين إن حكومة تكنولوجيا المعلومات : "هي استخدام مجموعة من البيانات من مبادئ و معايير وأهداف في وضع و رسمي سياسات و إجراءات لتحسين عمليات و أنشطة تكنولوجيا المعلومات و الرقابة عليها".

2. **أهمية حوكمة تكنولوجيا المعلومات:**

تظهر أهمية حوكمة تكنولوجيا المعلومات من خلال دورها في تحقيق **الأتي:** (عبدالرحمن, نجلاء إبراهيم يحيي، 2013، صفحة 223)

- تطوير استراتيجية تكنولوجيا المعلومات والبدء في المراجعة التشغيلية.
- تطوير إدارة نظم تقنية المعلومات، وتحديد الأساليب والوسائل والعمليات المرتبطة بتقنية المعلومات.
- تحديد أفضل الممارسات في مجال التطور التكنولوجي.
- إدارة تنمية و تطوير تطبيقات تكنولوجية المعلومات.
- ضمان فعالية خدمات تكنولوجيا المعلمات، لتوصيل الاستراتيجية إلى أقسام الأعمال.

3. **مقومات تطبيق حوكمة تكنولوجيا المعلومات:**

تتمثل مقومات نجاح تطبيق حوكمة تكنولوجيا المعلومات في أي منشأة فيما **يلي:**

- تشير إدارة البنية التحتية لتكنولوجيا المعلومات إلى القرارات المتعلقة بأنواع الأجهزة والبرامج وإنشاء الشبكات والبيانات المستخدمة داخل المنشأة، ومعايير تحقيق أصول تكنولوجيا المعلومات الخاصة بها وتطويرها.
- الموائمة بين الاستراتيجية العامة للمؤسسة وخطط التشغيل اللازمة لتحقيق أهداف الاستراتيجية وبين الخطة الاستراتيجية لتقنية المعلومات (عبدالرحمن, نجلاء إبراهيم يحيي، 2013، صفحة 225).
- وضع خطة مالية وتمويلية لتكنولوجيا المعلومات.
- وضع إطار عام لتطبيق الحوكمة والرقابة على تقنيات المعلومات مع مراعاة ما تصدره جهات الرقابة والتفتيش والقوانين المنظمة لعمل المؤسسات واختيار البدائل العملية المعروضة.
- القيام بتشكيل اللجان المتخصصة في توجيه تكنولوجيا المعلومات ووضع الاستراتيجية الخاصة بها، ويتعين ان يكون مستوى هذه اللجان من اعضاء مجلس الادارة.

4. إدارة مخاطر تكنولوجيا المعلومات

تعتبر تكنولوجيا المعلومات من أهم المجالات التي تتعرض للعديد من المخاطر، وقد حددت لجنة التكنولوجيا المنبثقة من الاتحاد الدولي للمحاسبين IFAC مخاطر نظم تكنولوجيا المعلومات الى ثلاثة أنواع رئيسية من المخاطر هي: (حجاز, عبد الفتاح بيومي;، 2006) :

- مخاطر البنية التحتية لنظم تكنولوجيا المعلومات.
- مخاطر تطبيق تكنولوجيا المعلومات.
- مخاطر تكنولوجيا المعلومات الخاصة بأعمال المنشأة.

وفى ضوء ذلك أوصى مراجعي نظم المعلومات ان تنشئ المنشآت وحدة إدارية للرقابة والإشراف على تطبيق واستثمار تكنولوجيا المعلومات في المنشآت يطلق عليها لجنة الاشراف على تكنولوجيا المعلومات. كما أوضحت جمعيه مراجعة رقابة نظم المعلومات(ISACA) . يجب على المؤسسات أن تشكل هذه اللجنة وفقاً للقواعد والقواعد التي تصدرها الجمعية باسم "أهداف الرقابة على المعلومات والتقنية ذات الصلة، والتي يكون فيها دورها الفعال في تنفيذ الخطة الاستراتيجية لتكنولوجيا المعلومات من أجل" التأسيس والرقابة والإشراف والاستثمار في ذلك لتحقيق هدف الشركة.

كما أنه تدعيما لإدارة مخاطر تكنولوجيا المعلومات. فإنه لابد من ضرورة تبنى المنشاة تخصيص قسم أو إدارة بحسب حجم الاستثمار في تكنولوجيا المعلومات فى المنشأة تكون مسئولة عن حماية أمن ونظم وتكنولوجيا المعلومات.

2. التشفير والتوقيع الإلكترونيين.

2.1. التشفير الإلكتروني

2.1.1 مفهوم التشفير الالكتروني:

التشفير هو: عملية دمج المعلومات في رمز سري غير مفهوم ثم كسر هذا الرمز بعد وصوله إلى خادم الويب الآمن، مما يعني أن التشفير هو استبدال مستند أو رسالة باستخدام برنامج معين، ولهذا فإن عملية التشفير تتضمن تحويل النصوص البسيطة إلى رموز (أحرف، أرقام، علامات). قبل إرسالها إلى مستقبلها شريطة أن يكون لهذا الأخير القدرة على حل الشفرة وتحويل الرسالة إلى صيغتها الأصلية باستخدام مفتاح التشفير (دوج, جيرلاش، 2001).

2.1.1 طرق التشفير الإلكتروني:

2.1.1.1 التشفير باستخدام المفتاح المتماثل (المفتاح السري):

يعتمد نظام التشفير المتماثل أو المتناظر على استخدام نفس المفتاح من طرف مصدر الرسالة والمرسل إليه للقيام بتشفير الرسالة وإعادة فك رموزها وذلك وفقا للخطوات **التالية:**

- في هذا النظام يتم استخدام المفتاح الخاص (السري) المستند إلى وضع رياضة معقدة (خوارزميات) في عملية استبدال البيانات برموز وحروف بغرض الحصول على رسالة مشفرة.
- يقوم المستقبل بعد تلقي الرسالة المشفرة بحل الرموز، وذلك باستخدام نفس المفتاح الخاص (كلمة المرور) الذي يملكه المرسل. حيث أنه تم الاتفاق مسبقا بين الطرفين على كلمة المرور التي تقوم برمجيات التشفير بتحويلها إلى ثنائي (اضافة إلى رموز أخرى) هو المفتاح الخاص.
- بعد استخدام المستقبل لكلمة المرور بتشكيل المفتاح الذي يقوم بتحويل الرسالة المستقبلة من صورتها المرمزة غير المقروءة وغير المفهومة إلى صورتها الأصلية الواضحة.

– إن عدم استغراق هذا النظام لوقت طويل وجهد كبير لتشفير encryption وفك تشفير البيانات decryption، ساهم كثيراً في حماية الرسائل المتنقلة من الاطلاع عليها، الا أنه يعترض استخدامه مشكلة آمن تبادل المفتاح السري فهو عرضه للسرقة بسبب عدم توفر وسيلة مؤمنة وخاصة لنقله، كما أنه في حالة تعامل المرسل مع عدد كبير من المستقبلين يتوجب عليه امتلاك الكثير من المفاتيح الخاصة بكل واحد منهم، اما اذا فضل المرسل استخدام مفتاح واحد فقط مع عدد من المستقبلين فإن ذلك يؤدي إلى شيوع المفتاح والإخلال بمبدأ السرية.

2.1.2.2 التشفير باستخدام المفتاح اللا متماثل (المفتاح العام).

أو ما يعرف بالتشفير اللامتماثل (Asymmetric Cryptography) .تم تطوير هذا النظام في السبعينات في بريطانيا وكان استخدامه حكراً على قطاعات معينة من الحكومة. ويعتمد في مبدأه

على وجود مفتاحين وهما المفتاح العام Public key والمفتاح الخا.Privet key حيث أن المفتاح العام هو لتشفير الرسائل والمفتاح الخاص لفك تشفير الرسائل. المفتاح العام يرسل لجميع الناس أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسله لأحد. فمن يحتاج أن يرسل لك رسالة مشفرة فإنه يستخدم المفتاح العام لتشفيرها ومن ثم تقوم باستقبالها وفك تشفيرها بمفتاحك الخاص (حجاز, عبد الفتاح بيومي;، 2006) .

إن ارتكاز نظام التشفير اللامتماثل على مبدأ عدم نشر المفتاح الخاص للجميع، ساعد على توفير حماية كبيرة للرسائل من التطفل عليها، إلا أن هذه السرية تتطلب الكثير من الوقت والجهد والمعدات المعقدة لإجراء عملية التشفير وفكها مما يجعل هذا النظام جد بطيء ومكلف مقارنة بالنظام السابق.

2.1.2.3. المزج بين اسلوبي استخدام المفتاح المتماثل والمفتاح العام:

يهدف هذا النظام إلى تفادي عيوب النظامين السابقين من خلال ضمان قدر كبير من الآمن والحماية للبيانات بأقل تكلفة و في اقصر وقت، و يستطيع هذا النظام تحقيق هدفه من خلال الجمع بين المفتاح المتماثل والمفتاح العام.

2.2 التوقيع الإليكتروني:

عرفت المادة (2 /ا) من القانون النموذجي المتعلق بالتوقيعات الإلكترونية و الذي و ضعته لجنة الأمم المتحدة لقانون التجارة الدولية سنة 2001 التوقيع الإلكتروني بانه "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، و يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات وبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات" (برهم, نضال اسماعيل، 2005). آي أن التوقيع الإلكتروني يتمثل في حروف و أرقام و اشارات مجموعة في ملف رقمي صغير يساعد على تمييز هوية الموقع و شخصيته دون غيره و بأنه هو من قام بإجراء المعاملة و تنفيذها.

2.2.1 أنواع التوقيع الإلكتروني:

2.2.1.1 التوقيع الرقمي أو الكودي.

وهو عبارة عن عدة أرقام يتم تركيبها لتكون فى النهاية كودا يتم التوقيع به، ويستخدم هذا فى التعاملات البنكية والمراسلات الإلكترونية التى تتم بين التجار أو بين الشركات وبعضها، ومثال لذلك بطاقة الائتمان التى تحتوي على رقم سرى لا يعرفه سوى العميل، ويعد هذا النوع وسيلة آمنة لتحديد هوية الشخص الذي قام بالتوقيع من خلال الحاسب الآلي (حجاز, عبد الفتاح بيومي;، 2006، صفحة 249)

2.2.1.2 التوقيع البيومترى.

ويقوم على أساس التحقق من شخصية المتعامل بالاعتماد على الصفات الجسمانية للأفراد مثل البصمة الشخصية، مسح العين البشرية التعرف على الوجه البشرى، خواص اليد البشرية، التحقق من نبرة الصوت،

والتوقيع الشخصي، ويتم التأكد من شخصية المتعامل عن طريق إدخال المعلومات للحاسب أو الوسائل الحديثة مثل التقاط صورة دقيقة لعين المستخدم أو صوته أو يده ويتم تخزينها بطريقة مشفرة فى ذاكرة الحاسب ليقوم بعد ذلك بالمطابقة. ويعترى هذا النظام العديد من المشاكل منها أن صورة التوقيع يتم وضعها على القرص الصلب للحاسب ومن ثم يمكن مهاجمتها أو نسخها بواسطة الطرق المستخدمة فى القرصنة الإلكترونية، كذلك عدم إمكانية استخدام هذه التقنية مع جميع الحاسبات المتوفرة، ويحتاج هذا النوع من التوقيع إلى استثمارات ضخمة لتمكين مستخدمي الشبكة الإلكترونية من استخدام الخصائص الذاتية لشخص الموقع فى التوقيع الإلكتروني (11، 2016)

2.2.1.3 **التوقيع بالقلم الإلكتروني.**

يقوم هنا مرسل الرسالة بكتابة توقيعه الشخصي باستخدام قلم إلكتروني خاص على شاشة الحاسب الآلي عن طريق برنامج معين ويقوم هذا البرنامج بالتقاط التوقيع والتحقق من صحته، ولكن يحتاج هذا النظام إلى جهاز حاسب آلي بمواصفات خاصة ويستخدم هذا بواسطة أجهزة الأمن والمخابرات كوسيلة للتحقق من الشخصية .وهذا النوع افضل من التوقيع اليدوي والذى يتم على شاشة جهاز الكمبيوتر أو على لوحة خاصة معدة لذلك باستعمال قلم خاص عند ظهور المحرر الإلكتروني على الشاشة، وهذا النوع لا يتمتع بأي درجة من الأمان كذلك لا يتضمن حجية في الإثبات (حجاز, عبد الفتاح بيومي;، 2006، صفحة 249)

3. **الشهادات الرقمية ونظام المعاملات الآمنة.**

3.1 **الشهادات الرقمية:**

لطالما تعرضت معاملات التجارة الالكترونية إلى اشكال عديدة من الخداع وانتحال الشخصيات ولكي يتم تجنب هذا الخداع لأبد من التحقق من هوية الاطراف المتبادلة للمعلومات وهذا باللجوء إلى شهادات رقمية تؤكد شخصية المتعاملين.

3.1.1 **مفهوم الشهادات الرقمية:** هي وثيقة رقمية تحتوي على مجموعة من المعلومات التي تقود إلى التحقق من هوية الشخص أو المنظمة أو الموقع الإلكتروني وتشفر المعلومات التي يحويها جهاز الخادم (server)عبر ما يسمى بتقنية .(SSL Layer sockecSsecurS) .يمكننا تشبيه الشهادة الرقمية بجواز سفر أو وثائق اعتماد رقمية تتم أثناء الاتصال بين الخادم (server) والعميل (client) .فحينما يريد العميل إرسال معلومات تتصف بالسرية أو الحساسية يقوم متصفح الانترنت و بشكل آلي بالدخول إلى جهاز خادم (server). خاص للتأكد من هوية الجهة التي يرغب في إرسال المعلومات إليها وبالتالي يضمن الحصول على قناة اتصال آمنة، وبهذا تساعد الشهادة الإلكترونية صاحبها على تحقيق شخصيته الإلكترونية واثبات صحة كافة معلوماته وضمان صدق العملية المطلوبة، وهو ما يؤدي إلى ضمان آمن التعاملات التجارية والفردية وبالتالي تطور وانتشار التجارة الإلكترونية. وتتضمن الشهادة الرقمية مجموعة من البيانات

والمعلومات الإلكترونية والتي قامت هيئة المواصفات القياسية العالمية iso بتحديدها و فقا للمعيار 509 – Xكالاتي: (غنيم, احمد محمد، 2004):

- بيانات عن المرسل تحدد هويته.
- نسخة من المفتاح العام للمرسل وتوقيعه الرقمي.
- رقم تسلسلي للشهادة وتاريخ انتهاء صلاحيتها.

إضافة إلى: الخوارزمية المستخدمة لإنشاء التوقيع اسم الجهة المصدرة للشهادة) هيئة التوثيق (الغرض من استخدام المفتاح العام الإصدار خوارزمية بصمة الإبهام بصمة الإبهام. (http://www.lahaonline.com، 2016).

فهناك الشهادات الرقمية الممنوحة للأفراد والمرفقة بمتصفحات الويب. وهناك الشهادات الإلكترونية الخاصة بالمؤسسات والتجار والموجودة على مستوى خادم الويب والتي تضمن الوجود الفعلي لهدا الموقع والنوع الأخير هي شهادات التوقيع الإلكتروني المستعملة لتأكد هوية صاحب الرسالة واثبات صحة توقيعه.

3.1.2 **أهمية الشهادات الرقمية**:

تساهم الشهادات الرقمية في تطوير التجارة الإلكترونية بشكل كبير من خلال تأكيدها لهوية الطرفين وضمانها لسرية المعاملات باستخدام تقنية التشفير حيث تحتوي كل شهادة على مجموعة من البيانات والمعلومات الموقعة بالمفتاح العام لصاحب الشهادة وكذلك المفتاح الخاص للهيئة المصدرة لهذه الشهادة فاذا نجح المستقبل في فك شفرة الشهادة باستخدام المفتاح العام للهيئة هذا يؤكد بان الهيئة الموقعة على الشهادة هي نفسها التي اصدرتها.

3.2 نظام المعاملات الإلكترونية الآمنة.

إن المشكل الرئيسي الذي تعاني منه التجارة الإلكترونية هو مشكل تامين الدفع و الاخطار التي قد تترتب عنه، فالدفع الإلكتروني باعتباره عملية مصرفية متعددة الاطراف و مفتوحة على فضاء دولي يمكنه أن يتعرض إلى صور عديدة من الاعتداءات والتي تخلق لدى المشتري هاجس ضمان و تامين عملية شراء السلع عبر الانترنت، كذلك للبائع الذي يرغب في ضمان قدرة الزبون على التسديد و لذلك تم التفكير في اللجوء إلى وسائل آمن حديثة قادرة على جعل الدفع أكثر فعالية وأكثر سرية و كذلك أكثر قدرة على حماية المستهلك و ضمان حقوق البائع، و من بين أهم هذه الوسائل نظام المعاملات الالكترونية الامنة "SET".

3.2.1 تعريف نظام المعاملات الإلكترونية الآمنة.

هو عبارة عن بروتوكول طورته مجموعة كبيرة من الشركات العالمية للائتمان كا فيزا وماستر كارد ووظيفته الاساسية هي توفير الأمان لمدفوعات البطاقات المصرفية (الائتمانية) اثناء عبورها الإنترنت بين حاملي البطاقات والتجار والبنوك (http://www.alriyadh.com/159573، 2016)

ويستطيع هذا البروتوكول ضمان آمن المعاملات المالية للبطاقات الائتمانية من خلال إصدار شهادات رقمية للمستهلكين والتجار تشهد بصحة هويتهم اثناء قيامهم بمعاملات التجارة الإلكترونية ويتم الاحتفاظ بهذه الشهادة في برمجيات المحفظة الإلكترونية والتي تحتوي بالإضافة إلى شهادة "SET" معلومات أخرى مثل رقم البطاقة الائتمانية و تاريخ انتهائها حيث يتم تخزين هذه المحفظة على كمبيوتر المستخدم ليتم استعمالها للقيام بعملية الدفع عبر الانترنت في أي وقت، و يسعى هذا البروتوكول إلى تحقيق مجموعة من الأهداف **تتمثل في:**

- تامين سرية المعلومات الخاصة بالدفع من خلال تقنية التشفير.
- المعلومات المحولة تكون كاملة وغير قابلة لاي تغيير بفضل استخدام التوقيع الإلكتروني.
- تحديد هوية صاحب البطاقة والتاجر فالشهادات الإلكترونية تضفي الكثير من الشرعية والموثوقية على الطرفين وتدل أن البنك قد تحقق من شخصيتهما.

3.2.2 مبدأ **عمل نظام المعاملات الإلكترونية الآمنة.**

يمكننا توضيح المراحل التي يتم بها استخدام نظام بروتوكول الحركات المالية الامنة من خلال الشكل:

1- يشترك الزبون لدى إحدى البنوك أو المؤسسات الائتمانية بغية الحصول على برنامج خاص ببروتوكول الحركات المالية الامنة (هو برنامج المحفظة الالكترونية التي تحتوي على البطاقة الائتمانية وشهادة إلكترونية) .

2- يفتح التاجر ايضا حسابا لذي أحد البنوك ويحصل على برمجيات لاستخدام بروتوكول (تشمل هذه البرمجيات شهادة set والمفتاح العام) .

3- يزور المشتري موقع البائع الذي يتعامل ببروتوكول set ويحدد حاجياته كما يستعمل الزبون المفتاح العام للتاجر من اجل تشفير معلومات طلب الشراء (الاصناف المطلوبة والكميات والقيمة) .

4- يستخدم الزبون المفتاح العام للتاجر من اجل تشفير معلومات الدفع (رقم بطاقة الائتمان والقيمة المدفوعة واسم البائع). كما يستخدم هذا الزبون محفظته الإلكترونية لإرسال المعلومات المالية المشفرة والشهادة الإلكترونية الى البائع.

5- يفك التاجر تشفير معلومات طلب الشراء باستخدام مفتاحه الخاص ويقوم بتوجيه المعلومات المالية المشفرة إلى البنك او شركة الائتمان.

6- يتحقق البنك من هوية البائع والمشتري (باستخدام الشهادات الرقمية) ويعالج معلومات الدفع ويرسل رسالة الموافقة على الصفقة إلى البائع ليقوم هذا الأخير بإتمام معاملات الصفقة وشحن البضاعة.

7- تتم عملية المقاصة بين بنك التاجر وبنك المشتري.

الخاتمة:

كانت هذه بعض النصائح التي نراها ضرورية لنتفادى جميعا شر الوقوع في عمليات النصب والاحتيال الموجودة في شبكة الانترنيت والتي أصبحت شائعة ومتعددة الأشكال والأساليب، حيث يستخدم المحتالون مواقع انترنت مزيفة، أو رسائل مضلّلة عن طريق البريد الالكتروني، وذلك بتقليد العلامات التجارية والشركات الموثوق بها، من أجل سرقة معلومات شخصية، مثل: أسماء المستخدمين، وكلمات السرّ، وأرقام بطاقات الائتمان ومعلومات الفواتير.

التوصيات والاستنتاجات: خلصت الدراسة إلى:

- تقوم الهيئات العالمية المختصة في مجال المعلوماتية بتطوير برمجيات الحماية الالكترونية عن طريق البحث عن الثغرات في الأنظمة والتطبيقات التي قد تفتح المجال للقراصنة للممارسة أعمال غير شرعية واستخدام أساليب تضليلية للاعتداء على أمن وخصوصية المعلومات الشخصية، وفي هذا الصدد تقوم هذه الهيئات بإدراك النقائص وتحيين البرامج قصد خاطر الاحتيال والغش المعاصرة.
- مستقبل التعامل الاقتصادي في الأوساط الالكترونية متوقف على مدى فعالية ونجاعة أساليب الوقاية الحديثة كون عنصر الأمان هو الركيزة الأساسية لقيام المبادلات التجارية وإجراء عمليات التسوية، فقيمة المعلومات التي تحافظ المنشآت على سريتها تعكس أبعادا مالية وخبايا استراتيجية قد تكون عاملا حاسما في تحديد مصيرها.

المصادر والمراجع:

11. (2016, 01 01). Retrieved from http://www.q8control.com/- .

-http://www.alriyadh.com/159573 . (10 01, 2016). *159573*. تم الاسترداد من ./http://www.alriyadh.com

-http://www.lahaonline.com. (09 01, 2016). *41544*. تم الاسترداد من .http://www.lahaonline.com

- الطاهر , علاء فرج. (2010). *الحكومة الإليكترونية بين النظرية والتطبيق*. عمان – الأردن: دار الراية.
- اللجنة الاقتصادية والاجتماعية لغربي آسيا, (الإسكوا) .(2013) *نشرة تكنولوجيا المعلومات والاتصالات للتنمية في الدول النامية* .نيويورك: الأمم المتحدة.
- المبيضيين, صفوان. (2011). *الحكومة الإليكترونية بين النظرية والتطبيقوالتجارب الدولية*. الأردن: دار البازوري.
- المنتدى الاقتصادي العالمي. (2014). *المكاسب والمخاطر في البيانات الضخمة* . نيويورك: التقرير العالمي لتكنولوجيا المعلومات – wefch/gitr14.

- الهياجة, أحمد الفخري. (بلا تاريخ). *إدارة مشاريع الحكومة الإليكترونية تجارب عربية وعالمية* . تم الاسترداد من المعهد العربي لإنماء المدن.
- برهم, نضال اسماعيل. (2005). *احكام التجارة الالكترونية*. الأردن: دار الثقافة للنشر و التوزيع.
- حجاز, عبد الفتاح بيومي;. (2006). *التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر و الانترنت*. الاسكندرية: دار الفكر الجامعي.
- حجازي, نبيل علي; حجازي, نادية ;. (2005). *رؤية عربية لمجتمع المعرفة*. الكويت: المجلس الوطني للثقافة والفنون والأداب.
- دوج, جيرلاش. (2001). *الاستثمار عبر الانترنت ", ترجمة تيب توب لخدمات التعريب و الترجمة,*. مصر: دار الفاروق للنشر و التوزيع.
- عبدالرحمن, نجلاء إبراهيم يحيي. (2013). تكنولوجيا المعلومات في ضبط مخاطر المنشأة في القطاع المصرفي السعودي. *مجلة الفكر المحاسبي، 17*، 222.
- عوض, أمال محمد. (2008). دور آليات الحوكمة في تعزيز حوكمة تكنولوجيا المعلومات وضبط مخاطر الأنشطة الاليكترونية للمنشآت. *مجلة الدراسات المالية والتجارية – كلية التجارة ،جامعة بني سويف*.
- غنيم, احمد محمد. (2004). *" الادارة الالكترونية، افاق الحاضر و تطلعات المستقبل"*. مصر: المكتبة المصرية، المنصورة.
- مجموعة البنك الدولي. (2016). *تقرير عن التنمية في العالم – العوائد الرقمية*. واشنطن: openknowledge.worldbank.org.

وزارة تطوير القطاع العام. (2015). *أبرز المؤشرات الدولية وواقع حال الأردن فيها*. عمان: وزارة قطاع عام – الأردن.